


Securing VoIP

CSH6 Chapter 34
“Securing VOIP”
Christopher Dantos &
John Mason




1

Copyright © 2016 M. E. Kabay. All rights reserved.

Topics

- Introduction
- Regulatory Compliance & Risk Analysis
- Technical Aspects of VOIP Security
- Protecting the Infrastructure
- Encryption
- Concluding Remarks




2

Copyright © 2016 M. E. Kabay. All rights reserved.

Introduction

- Terminology:
 - ❑ Voice over Internet Protocol – VoIP
 - ❑ Internet Protocol Telephony – IPT
 - ❑ Shift to Unified Messaging Systems (UMS)
 - ✓ Instant messaging
 - ✓ Text messaging (to phones)
 - ✓ Voice communications
 - ✓ Video conferencing
 - ✓ E-mail
 - ✓ Network connectivity
- Significant benefits
 - ❑ Telework
 - ❑ Cost reductions



3

Copyright © 2016 M. E. Kabay. All rights reserved.

Regulatory Compliance & Risk Analysis

- Key Federal Laws & Regulations
- Other US Federal Laws & Regulations
- State Laws & Regulations
- International Laws & Considerations
- Liability
- Risk Analysis




4

Copyright © 2016 M. E. Kabay. All rights reserved.

Key Federal Laws & Regulations

- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability & Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Regulations from
 - ❑ Securities & Exchange Commission (SEC)
 - ❑ Health & Human Services (HHS)
 - ❑ Federal Trade Commission (FTC)
- General requirements
 - ❑ Mandated protection for consumer & patient personally identifiable information (PII)
 - ❑ Periodic management testing of internal controls
 - ❑ Continuous process improvement (policies, tests, reports)




5

Copyright © 2016 M. E. Kabay. All rights reserved.

Other US Federal Laws & Regulations: E911

- Enhanced 911 (E911)
- Federal Communications Commission (FCC)
- Mobile phones must process 911 calls
- Allow geolocation
- Phase I: report location of *antenna* receiving 911 call
- Phase II: report location of *phone* ±50-300m
- Not required for VoIP used for internal business only




6

Copyright © 2016 M. E. Kabay. All rights reserved.

Other US Federal Laws & Regulations: CALEA (1)


- Communications Assistance for Law Enforcement (CALEA)
- Interception of call content (wiretap)
- Discovery of call-identifying information (dialed-number extraction)
- Requires telecoms to support legal demands for info
- Packet Technologies & Systems Committee (PTSC)
 - ❑ Lawfully Authorized Electronic Surveillance (LAES) for VoIP Technologies
 - ❑ Part of Wirelines Telecommunications Networks, V2 (Rev T1.678-2004)





7

CALEA (2)

- Telecommunications Industry Association (TIA)
 - ❑ Standard J-STD-025-B
 - ❑ Surveillance of CDMA2000 broadband access
- Wireless Technology & Systems Committee (WTSC)
 - ❑ Alliance for Telecommunications Industry Solutions (ATIS)
 - ❑ Standard T1.724
 - ❑ Surveillance of GPRS/UMTS broadband access





 

8

CALEA (3)

- FCC's role
 - ❑ §102: FCC has authority to identify communications services subject to CALEA
 - ❑ §103: carrier must ensure compliance with access
 - ❑ §105: FCC must define security & integrity regulations
 - ❑ §109: FCC must refine *reasonable achievability* of goals
- Key issue: who is responsible for compliance?
 - ❑ CALEA refers to common carriers for hire
 - ❑ What about internal VoIP service for 1 organization?
 - ❑ Some interpretations (still under debate) suggest that even internal networks subject to CALEA
 - ❑ Discuss with attorneys specializing in FCC law





9

State Laws & Regulations

- All US states have laws governing surveillance
 - ❑ 31 address computers
 - ❑ 14 address mobile phones
- Organization & legal departments must consult experts in network law for specific jurisdiction(s)
- National Conference of State Legislators (NCSL)
 - ❑ Links to applicable laws of each state
 - ❑ Summary of coverage
 - ❑ See "Electronic Surveillance Laws" for table of links


<http://www.ncsl.org/default.aspx?tabid=13492>
(checked 31 Oct 2011)

International Laws & Considerations

- International picture varies extensively
 - ❑ Consult local attorneys specializing in communications law for specific jurisdictions
- European Privacy Directive
 - ❑ http://ec.europa.eu/justice/data-protection/index_en.htm
 - ❑ "Everyone has the right to protection of personal data"
 - ❑ "Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose."
 - ❑ "Furthermore, persons or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law."
 - ❑ Text of EPD at < <http://tinyurl.com/3d5hup2> >

Liability


- Criminal penalties & civil penalties possible in US
 - ❑ Federal prosecution takes precedence over state
 - ❑ Fines >\$500 per violation
 - ❑ Max (\$100/day of violation or \$10K)
- Violations of SOX, GLBA, HIPAA
 - ❑ ≤ \$250K
 - ❑ Imprisonment
 - ❑ Adverse findings on SOX annual control assessment
 - ❑ Stock delisting (SOX)
 - ❑ Additional regulatory reviews (SOX)
 - ❑ Additional SOX-related attestations



12

Risk Analysis (1): SOX


- Most important: effect on financial statements
- Threshold uncertain: e.g., 5% of net income
- Resolve differences quickly among external & internal financial auditors
- Risk control matrix
 - ❑ Identify & describe key / primary controls
- Segregation of Duties (SoD) matrix
 - ❑ Employee activities / roles / functions
 - ❑ Acceptable / not acceptable
 - ❑ Stimulate thinking about VoIP management



13

Risk Analysis (2): SOX cont'd

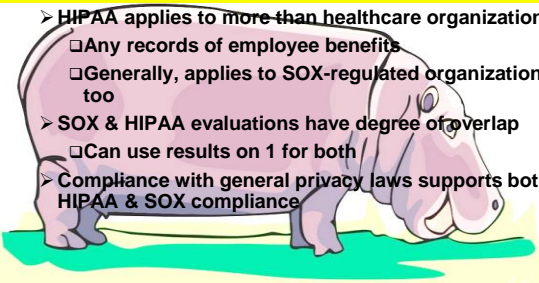
- Sample matrix for monitoring VoIP (and other) technologies (P 34-7):
- Be aware that SOX testing may rule any error a failure in VoIP implementation
 - Level of financial risk associated with the control or area
 - Control objectives
 - Control or business application owner(s)
 - Related tests
 - Testing status
 - Test results
 - Deficiency and remediation status and follow-up
 - Compensating controls
 - Executive-level "dashboard" for status
 - Other related information



14

Risk Analysis (3): HIPAA*

- HIPAA applies to more than healthcare organizations
 - ❑ Any records of employee benefits
 - ❑ Generally, applies to SOX-regulated organizations too
- SOX & HIPAA evaluations have degree of overlap
 - ❑ Can use results on 1 for both
- Compliance with general privacy laws supports both HIPAA & SOX compliance




***NOT "HIPPA"!**

15

Risk Analysis (4): Privacy Laws

- Particularly well-known:
 - ❑ GLBA
 - ❑ California SB1386
- Emphasis
 - ❑ Unauthorized access or disclosure
 - ❑ Consumer information
- Encryption for VoIP
 - ❑ Safe harbor under CA statute for encrypted info
 - ❑ But no mandated level of encryption
 - ❑ Transmission encryption not required
 - ❑ Assess issues at time of implementation
 - ❑ Continue to monitor regulatory environment




"I'll need you to sign this full nondisclosure agreement."

16

Technical Aspects of VOIP Security

- Protocol Basics
 - ❑ Audio Stream Protocols: RTP & UDP
 - ❑ Signaling Protocols: SIP & H.323
- VoIP Threats
 - ❑ SPIT
 - ❑ Eavesdropping
 - ❑ Theft of Service
 - ❑ MIMA



17

Audio Stream Protocols

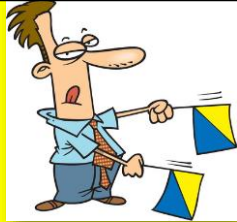
- RTP: Real-time Transport Protocol
 - ❑ Base for almost all VoIP
- UDP: User Datagram Protocol
 - ❑ Similar to TCP: layer-4 network communications
 - ❑ Less overhead (delay) than TCP
 - ❑ But loses more packets
 - ❑ Up to 10% packet loss undetectable by users

Application (7)	Provides services directly to user applications. Because of the potentially wide variety of applications, this layer must provide a wealth of services. Among these services are establishing primary mechanisms, authenticating the intended communication partners, and determining if adequate resources are present.
Presentation (6)	Performs data transformations to provide a common interface for user applications, including services such as reformatting, data compression, and encryption.
Session (5)	Establishes, manages, and ends user connections and manages the interaction between end systems. Services include such things as establishing communications as full or half duplex and grouping data.
Transport (4)	Insulates the three upper layers, 5 through 7, from having to deal with the complexities of layers 1 through 3 by providing the functions necessary to guarantee a reliable network link. Among other functions, this layer provides error recovery and flow control between the two end points of the network connection.
Network (3)	Establishes, maintains, and terminates network connections. Among other functions, standards define how data routing and relaying are handled.
Data Link (2)	Ensures the reliability of the physical link established at Layer 1. Standards define how data frames are encapsulated and provide necessary flow control and error handling at the frame level.
Physical (1)	Controls transmission of the raw bitstream over the transmission medium. Standards for this layer define such parameters as the amount of signal voltage swing, the duration of voltages (bits), and so on.

18

Signaling Protocols

- SIP: Session Initiation Protocol
 - ❑ Interactive multimedia sessions between users
 - ❑ VoIP, video conferencing, online games
 - ❑ Most commonly used protocol for VoIP
- H.323
 - ❑ Supports older, analog telecommunications gear
 - ❑ Used in enterprise installations for VoIP & video calls
- Call initiation
 - ❑ VoIP sets up call using SIP or H.323
 - ❑ Exchange control parameters (e.g., encryption, compression algorithms)
 - ❑ RTP packetizes voice data
 - ❑ UDP packet add addressing & sequencing data
 - ❑ Receiver uses "jitter buffer" to assemble packets



19

VoIP Threats (1)

- SPIT: SPam over Internet Telephony
 - ❑ Not yet major issue
 - ❑ No obvious method for sending e-mail to multiple VoIP targets
- Eavesdropping
 - ❑ Easy for unsecured communications using tools such as Ethereal
 - ❑ But only with access to terminators of connection (initiator / receiver)
- Theft of Service
 - ❑ Routing long-distance calls through VoIP equipment
 - ❑ Owners liable for telecommunications charges



20

VoIP Threats (2): MIMA

- Man-in-the-middle attacks
- VoIP vulnerable if without encryption
- Harm
 - ❑ Impersonate victim in fraud calls
 - ❑ Transfer inbound calls to wrong destination
 - ❑ Introduce fraudulent content in call
 - ✓ Including collecting phonemes & generating fake but realistic impersonation with fraudulent information
 - ✓ Could be serious problem for 911 calls



21

Protecting the Infrastructure

- Real-Time Antivirus Scanning
- Application Layer Gateways & Firewalls
- Logical Separation of Voice & Data
- Quality of Service
- Device Authentication
- User Authentication
- Network Address Translation & NAT-Traversal



22

Real-Time Antivirus Scanning

- Problem: normal AV measures may slow down packet processing
- RTAV may introduce jitter into voice-stream
- Do not allow VoIP admins to disable RTAV



23

Application Layer Gateways & Firewalls

- VoIP systems may have connections to important (and vulnerable) servers
 - ❑ E-mail & central authentication
 - ✓ RADIUS*
 - ✓ Active Directory
 - ❑ Database systems
 - ✓ Call logging
 - ✓ Call recording
- Apply application layer gateways (ALGs) to segregate VoIP servers from rest of production systems
- Some firewalls are SIP/VoIP-aware



24 *Remote Authentication Dial-In User Service

Logical Separation of Voice & Data

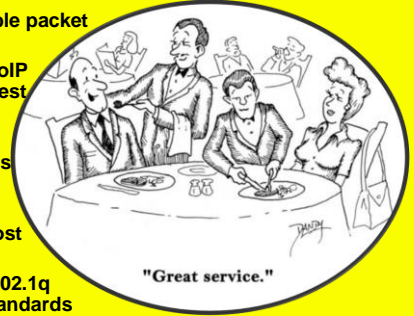
- Ideally, VoIP system completely separate from other production systems
- But expense may be too high
 - ❑ Separate cables (!)
 - ❑ Separate network equipment
- But define VoIP subnet
 - ❑ DHCP* request from user process or handset
 - ❑ Distribute IP addresses using hardware ID
 - ❑ Distinct addresses allow effective firewall screening



25 *Dynamic Host Configuration Protocol

Quality of Service (QoS)

- Define acceptable packet delay / loss
- Can prioritize VoIP packets for fastest processing
- Some VoIP-enabled firewalls keep packet buffers
 - ❑ Retransmit lost packets
- IEEE 802.1p & 802.1q provide QoS standards
 - ❑ See <http://ieee802.org/1/>



26 Copyright © 2016 M. E. Kabay. All rights reserved.

Device Authentication

- Store MAC addresses on VoIP server
 - ❑ Authenticate all SIP requests using list
- Configure VoIP devices automatically
 - ❑ Connect VoIP phone handsets without configuration
 - ❑ Apply image of proper configuration through network



27 Copyright © 2016 M. E. Kabay. All rights reserved.

User Authentication

- User management
 - ❑ Track calls, usage
 - ❑ Assign users to functional groups
 - ✓ Allow restrictions / privileges for destinations
- Technical
 - ❑ Usually connect VoIP infrastructure to LDAP* or Active Directory
 - ❑ Central authentication of users
 - ❑ Facilitate forwarding voicemail to computer or mobile phone
- Problems:
 - ❑ Authentication interval should be ~24 hours
 - ❑ Be sure to disable default accounts & passwords!



28 *Lightweight Directory Access Protocol

Network Address Translation & NAT-Traversal

- NAT
 - ❑ Used by firewalls & routers
 - ❑ Allow multiple devices to share single IP address
 - ❑ Firewall translates internal address into single IP address
 - ❑ Return packets interpreted by firewall to reach right device
- Problem: SIP reads translated address as real
 - ❑ Return stream using RTP/UDP can't get through firewall
- Workarounds
 - ❑ Configure NAT to support VoIP
 - ❑ Use unsecured (open) ports (but watch out for glitches)
 - ❑ VoIP proxy servers



29 Copyright © 2016 M. E. Kabay. All rights reserved.

Encryption: Critical Role


- Secure SIP
- Secure Real-Time Protocol
- Session Border Control



30 Copyright © 2016 M. E. Kabay. All rights reserved.

Secure SIP


- Transport Layer Security (TLS)
 - ❑ IETF
 - ❑ Secure & encrypt data communications
 - ❑ On public networks
 - ❑ Replace Secure Sockets Layer (SSL)
- Protocol
 - ❑ Handshake & record
- Secure SIP (SSIP)
 - ❑ Sends signaling messages over encrypted TLS channel
 - ❑ SIP proxy requests TLS session
 - ❑ Proxy returns certificate to SIP client for authentication
 - ❑ Client & proxy exchange encryption keys



31 Copyright © 2016 M. E. Kabay. All rights reserved.

Secure Real-Time Protocol (SRTP)


- Enhanced RTP
 - ❑ Encryption uses AES for stream cipher
 - ❑ Authentication
 - ❑ Integrity
- Blocks replay attacks
 - ❑ HMAC-SHA1*
 - ❑ MAC calculated using SHA hash + private key
 - ❑ Complies with Federal Information Processing Standards (FIPS)



32 *Hashed Message Authentication Code – Secure Hash Algorithm 1

Session Border Control (SBC)


- Services addressing VoIP
 - ❑ Security issues
 - ❑ QoS
 - ❑ NAT traversal (NAT-T)
 - ❑ Network interoperability
- Functions
 - ❑ Real-time bandwidth statistics
 - ❑ Can use to allocate network resources for QoS
 - ❑ Supports NAT-T algorithms for use of public networks with anonymity of internal resources
 - ❑ Accommodates SIP & H.3232



33 Copyright © 2016 M. E. Kabay. All rights reserved.

Concluding Remarks

- Architecture must protect against
 - ❑ Interception
 - ❑ Deception
 - ❑ Denial of service
- Continue to monitor field for new attack methodologies



34 Copyright © 2016 M. E. Kabay. All rights reserved.

Now go and study

35 Copyright © 2016 M. E. Kabay. All rights reserved.